

Protecting Server Data in Remote and Branch Offices

EXECUTIVE SUMMARY

Protecting critical business information stored on servers at remote and branch offices presents unique challenges to those responsible for protecting data all the way to the “edge of the network.” The pervasive use of computer resources throughout business operations not only continues to increase the volume of business data, but also its importance to achieving the specific mission of remote and branch offices. Ensured, rapid access to this data is as important to the success of the thriving remote or branch office as data center resources are to business headquarters.

Further, increasing regulations place greater scrutiny, and potential penalties, on data protection and recovery. Complicating data protection is the fact that it is widely distributed on file/print, email and database servers, with mobile technologies promoting the migration of mission-critical and sensitive information far outside the control and resources of centralized data centers.

Challenges faced by those responsible for protecting data in remote and branch offices often include:

- Difficulty extending Recovery Point Objectives (RPOs) and Recovery Time Objectives (RTOs) to remote and branch office data without incurring an expensive loss in staff productivity.
- The desire to have technical staff focused on more value-driven tasks rather than routine backup chores.
- The struggle to meet compliance regulations requiring the use of “commercially reasonable means” to protect and preserve all confidential data, wherever it is located, using limited technical staff in remote and branch offices.
- Limited options for ways to reliably move data off-site so that it is protected from disaster within commercially reasonable means — but easily recovered when needed.
- No easy way to control all the servers in remote offices across a multi-location business or enforce standardization of backup policies.

This paper presents a framework to assist in examining current methods of protecting server data in remote and branch offices — as well as the solutions designed to optimize server data protection programs, including:

- Common goals for protecting critical business data on servers — whether they are inside or outside the data center
- The differences between traditional backup solutions appropriate for server data protection within the data center — and the very different needs of remote server protection in offices far outside the data center
- Disk-based backup with integrated online services as a viable alternative to traditional backup solutions for remote server data protection
- Key characteristics for evaluating disk-based backup with integrated online services for remote and branch offices

Finally, this paper outlines the next steps in evaluating an online disk-based backup solution for remote and branch offices.

DOCUMENT INFORMATION

Protecting Server Data in Remote and Branch Offices

PRINTED

January 2007

COPYRIGHT

Copyright © 2007 Iron Mountain Incorporated. All Rights Reserved.

TRADEMARKS

Iron Mountain and the design of the mountain are trademarks or registered trademarks and Iron Mountain Digital is a trademark of Iron Mountain Incorporated. All other trademarks and registered trademarks are the property of their respective owners.

CONFIDENTIALITY

The information set forth herein represents the confidential and proprietary information of Iron Mountain. Such information shall only be used for the express purpose authorized by Iron Mountain and shall not be published, communicated, disclosed or divulged to any person, firm, corporation or legal entity, directly or indirectly, or to any third person without the prior written consent of Iron Mountain.

DISCLAIMER

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of Iron Mountain Inc. The information in this document is subject to change without notice and should not be considered a commitment by Iron Mountain Inc. While Iron Mountain has made every effort to ensure the accuracy and completeness of this document, it assumes no responsibility for the consequences to users of any errors that may be contained herein.

TABLE OF CONTENTS

	Page
COMMON GOALS FOR PROTECTING CRITICAL BUSINESS DATA ON SERVERS	4
PROTECTING DATA <i>WITHIN</i> THE DATA CENTER — EVOLVING TAPE-BASED SOLUTIONS ...	5
Staffing and tools to manage tape-based solutions?	5
Off-site tape vaulting services	5
Evolution of hybrid solutions	6
PROTECTING REMOTE SERVER DATA <i>OUTSIDE</i> DATA CENTERS — DIFFERENT NEEDS, DIFFERENT RESOURCES	6
Volume of server data	6
Fewer trained technical staff	6
Vulnerability from backups that remain on-site	6
DISK-BASED BACKUP AND RECOVERY WITH INTEGRATED ONLINE SERVICES — A VIABLE ALTERNATIVE FOR REMOTE AND BRANCH OFFICES	7
What are they?	7
More than just backup and recovery	7
Methods of implementation	7
KEY CHARACTERISTICS FOR THE REMOTE AND BRANCH OFFICE IN EVALUATING DISK-BASED BACKUP WITH INTEGRATED ONLINE SERVICES	7
Comprehensive and reliable data protection	7
Ease of use	8
Efficiency and speed	9
Highly secure communications and storage	9
Vendor expertise and flexibility	9
NEXT STEPS IN EVALUATING DISK-BASED BACKUP FOR REMOTE AND BRANCH OFFICES	10
Review your data protection strategy	11
Check out online resources	11
Use the checklist	11

ABOUT IRON MOUNTAIN DIGITAL

Iron Mountain Digital is the world's leading provider of data backup/recovery and archiving software as a service (SaaS). The technology arm of Iron Mountain Incorporated offers a comprehensive suite of data protection and e-records management software and services to thousands of companies around the world, directly and through a world-wide network of channel partners. Iron Mountain Digital is based in Southborough, Mass. with European headquarters in Frankfurt, Germany. For more information, visit www.ironmountain.com/digital.

Iron Mountain's LiveVault, our automated server backup and recovery solution, received a 2006 CoDiE Award in the Best Storage Software Solution category. LiveVault is offered as licensed software and managed service and features all of the key characteristics on the checklist provided in this paper. In addition, our PC backup and recovery services and products protect and defend data stored locally on desktops and mobile devices.

COMMON GOALS FOR PROTECTING CRITICAL BUSINESS DATA ON SERVERS

Today's businesses depend on access to their own information not only to succeed in the marketplace, but first and foremost, to survive in it. The pervasiveness of computing resources in the operations of the business makes fast access to critical business data imperative. Loss in productivity from downtime is expensive, regardless of the size and resources of the business — whether it's in the headquarters data center or in a thriving remote or branch office.

Picture the challenge to a branch office of a large law firm whose server crashes during the preparation of a brief for a strategically important trial the next day; a disruption in the access of a booming individual hotel property to its bookings and sales information; or the implications of losing strictly regulated financial data at a regional bank to man-made and natural disasters. Ensured, rapid access to data at remote and branch offices is critical to their individual success — and, in aggregate, to the business as a whole. Conversely, imagine the total cost in lost productivity of downtime and time-consuming recovery efforts from inadequate data protection strategies.

All businesses need to develop strategies and seek solutions to protect access to their data to achieve these fundamental business goals:

1. Mitigate risk and safeguard their business continuity
2. Demonstrate the ability to successfully and rapidly recover from disasters
3. Control unnecessary costs, from downtime to non-compliance fines and litigation costs, to additional IT resources/time
4. Avoid other penalties of non-compliance (prosecution, damage to reputation/brand)

A number of drivers challenge businesses of all sizes in achieving these goals. The sheer volume of business data on various types of servers (file and print servers, email and database servers) continues to increase, as does its assessed value (as much as \$1 million per 100 megabytes, according to the valuation of many companies').

In addition, this increased volume is being more widely distributed and migrating much more quickly. The growing use of mobile devices by a more virtual workforce increases the potential for data loss and misplacement during efforts to create comprehensive backups of the total information inventory of any single business — to say nothing of increased opportunity for security breaches and data theft.

Rising public awareness of information privacy violations and recent scandals in business governance have increased government and non-governmental regulations mandating compliance with corporate controls and accountability throughout the information lifecycle. Examples include HIPAA, Sarbanes-Oxley, Gramm-Leach-Bliley and regulations from the FDIC, SEC and NASD as well as at the state level. Compliance

CHALLENGES TO DATA PROTECTION

- The CERT/CC estimates that security events rose from approximately 21,000 in 2000 to more than 5 times that amount in 2003 — and that for every reported event, about four more go unreported
- Penalties for non-compliance with regulations to protect consumer and confidential data range from \$1-15 million in fines to up to 10 years in prison
- A 2005 survey shows that businesses continue to invest in perimeter security devices rather than safeguards for business-critical systems and data
- 30% of businesses do not include storage infrastructure in their corporate security policies and procedures

Source: *Best Practices to Secure and Protect Backup Data*, published by Iron Mountain in partnership with ESG and GlassHouse, 2005.

¹ Based on estimates compiled by companies like Contingency Planning Research and Strategic Research Corporation on how businesses value their data and the impact of its loss.

is just one of the issues increasing the complexity of managing various classes of critical business information throughout its lifecycle — from mission-critical for business continuity to non-current but legally required data. Many regulations require commercially reasonable protection to extend to data regardless of where it resides — from the data center to the edge of the network.

To stay ahead of these challenges, businesses need to develop successful data protection strategies and find the right solutions that address each of the four key steps in any data protection workflow — whether within the headquarters data center or outside of it in remote offices with no data center at all. Failure at any one of these steps can jeopardize business continuity, whether a business is protecting data from two servers — or two hundred. These key steps include:

1. *Backup* or replication of critical data on another device
2. *Removal* of replicated data to an off-site location to protect it against man-made or natural disasters
3. *Storage* of replicated data that both protects and organizes data so that it can be easily and quickly recovered
4. *Recovery* of replicated data from storage whenever and wherever needed

PROTECTING DATA WITHIN THE DATA CENTER — EVOLVING TAPE-BASED SOLUTIONS

Large companies managing terabytes of server data within their data centers have made significant investments over the years in tape-based data backup and recovery solutions, as well as the staffing and infrastructure to support them. While they require sufficient resources to manage and maintain, tape backup solutions used in conjunction with off-site tape vaulting services remain one of the least expensive ways for larger companies to store huge volumes of backup data — not only for disaster recovery purposes but, increasingly, to comply with regulatory requirements.

Staffing and tools to manage tape-based solutions: Within the data center, trained IT staff long familiar with tape-based backup manage the tasks associated with these solutions: tape cataloging, moving tapes off-site, reviewing logs, troubleshooting, locating tapes for a restore of data, etc. As these tape-based systems have matured, many data centers have purchased commercially available tools designed to help control the human error and hardware issues inherent in managing large tape backup operations.

Off-site tape vaulting services: To more effectively and efficiently address other steps in their data protection workflow, companies using tape-based solutions often employ the services of off-site tape vaulting services. A recent study conducted by *Storage Magazine* revealed that only 37% of businesses actually test their internal backups regularly, and of those that did, an alarming 77% found they were unable to fully recover data. Off-site tape vaulting services relieve the burden of tape cataloging and offer online tape inventory management tools to help ensure fast delivery times whenever and wherever companies need to recover backup data. They schedule regular inspection of media to ensure its integrity, providing better protection against the dangers of media failure (damaged or corrupted tapes). Off-site tape vaulting services test and ensure the recovery of critical data in case of disaster — important in demonstrating compliance with regulations on information storage and protection.

Evolution of hybrid solutions: With the introduction of new disk storage technologies, backup strategies have evolved to take advantage of both disk and tape-based solutions. Many larger companies are moving to hybrid technologies that combine disk-based solutions with existing tape backup processes. Disk-to-disk-to-tape² solutions and Virtual Tape Libraries³ both allow companies to increase the performance of backups by writing to disk during a convenient time (e.g., evening backup windows) and then writing to tape from the disk rather than from the production server. Hybrid solutions may offer faster restoration of recent history because they cache it locally.

PROTECTING REMOTE SERVER DATA *OUTSIDE* DATA CENTERS — DIFFERENT NEEDS, DIFFERENT RESOURCES

Data center managers responsible for data protection and disaster recovery across their businesses are often disappointed with their attempts to extend tape-based data protection and disaster recovery solutions out to the edge of the network. There are significant differences between the data protection workflow inside the data center or a centralized location and that of the remote or branch office:

- **Volume of server data.** As discussed previously, it's the storage cost of their terabytes of data that drives continued investment tape backup technology by larger companies. In contrast to managing terabytes of data, most remote and branch offices measure their data in gigabytes, not terabytes, running on low transaction file servers, Exchange and proprietary database servers.
- **Fewer trained technical staff.** Staffing typically includes few (if any) trained IT staff. Data protection responsibilities may be assigned to “generalists” ranging in rank from the principal of the business to administrative support staff. They typically work with less than well-defined processes and often lack cycles for the labor required given the balance of their other duties. It takes significant time to complete nightly backups (let alone more frequent backups) or effect full-scale recovery with technologies like tape-based solutions. Evaluating the success of a backup and troubleshooting results require expertise that may not be available on staff. Backup may not be perceived as a strategic, value-added activity — if not given the attention it requires, backups may be being neglected or forgotten.
- **Vulnerability from backups that remain on-site.** The lower volume of data previously cited may also limit the options for moving remote server backup data off-site — as well as adding yet another step to the workload of limited staff. As long as it is on-site, this data remains vulnerable to both man-made and natural disasters (including human error).

When these factors characterize a remote or branch office's data protection workflow, tape-based solutions are unlikely to be a good fit in achieving compliant or even acceptable data protection goals — yet their need for adequate data protection and avoidance of expensive downtime is every bit as critical as for their headquarters. Remote and branch offices require one, low-overhead solution that addresses each step in their data protection workflow — backup, removal, storage and recovery — and does so effectively within the office's resource constraints.

² In disk-to-disk-to-tape solutions, large companies increase the performance of backups by using a disk backup device to store from days to about a week of short-term data before sending it to tape for off-site storage and archiving. Obviously, during the time this data resides on the disk, these companies also achieve faster restoration of this short-term data, depending on the quality of the disk-based solution.

³ Virtual Tape Libraries allow businesses to keep a few days worth of backups on disk locally, as well as offload tape writing from the production servers. VTLs use traditional backup software to backup full data files to disk instead of tape (the software sees the disk as a tape autoloader and, subsequent to writing data to these disk devices, the software then writes it out to tapes which are then transported off-site).

DISK-BASED BACKUP AND RECOVERY WITH INTEGRATED ONLINE SERVICES — A VIABLE ALTERNATIVE FOR REMOTE AND BRANCH OFFICES

Given the challenges of implementing a tape-based solution and the characteristics of the data protection workflow in remote offices, an attractive alternative is offered by solutions featuring disk-based backup and recovery with integrated online services.

What are they? As their name implies, these integrated solutions combine a local disk device with an online backup and recovery service accessed through a broadband Internet or WAN connection. Backups occur automatically on a nearly continuous and/or scheduled basis, depending on the solution. Data is compressed, encrypted and transmitted to an off-site data storage vault, and optionally, an on-site disk backup appliance. Data restores can occur online or from the local disk backup appliance.

These solutions not only relieve staff of the effort of learning complex procedures and the time to manage additional technologies like tape or tape-disk hybrids, but they also make the process of backup and recovery automatic: “set-it-and-leave-it.” The quality of backup and recovery in the use of disk-based systems is higher as well — in contrast to the *Storage Magazine* study cited previously, 83% of the businesses recently surveyed by the Enterprise Strategy Group indicated that 80-100% of their disk-based backups and recoveries are successful. Disk-based systems that allow more continuous backup promote faster, timelier recovery with less data loss.

In addition to increased reliability and ease of use, lower costs for both disk technology and bandwidth are helping to accelerate the adoption of online backup and recovery solutions.

More than just backup and recovery. One of the biggest benefits these solutions offer to remote and branch offices is that they address not only backup and recovery, but their online capabilities also reduce the burden of removing the data and storing it safely off-site, protecting it from local disasters. Online disk-based backup and recovery solutions simplify *all* steps in the data protection workflow, providing a higher level of reliability, productivity and cost containment throughout the entire process.

Methods of implementation. Solutions for disk-based backup with integrated online services can be implemented in two ways:

1. Remote and branch offices with T1 lines can subscribe to these solutions offered as managed services by reliable third parties. This allows them to work within their resource constraints, leveraging the service provider’s investment in technology and storage resources while enjoying local control and rapid recovery.
2. Data centers in multi-location companies can install solutions offered as licensed software products and offer disk-based backup as an online service to their own remote offices. Note: Data centers gain an additional benefit from this product in backing up certain categories of their own critical data to disk for improved RTO/RPO, an example of the hybrid disk-based technology mentioned previously.

KEY CHARACTERISTICS FOR THE REMOTE AND BRANCH OFFICE IN EVALUATING DISK-BASED BACKUP WITH INTEGRATED ONLINE SERVICES

Below are some of the key characteristics to look for when evaluating online disk-based backup and recovery solutions to protect your server data — along with a checklist to help you separate the “best” from “the rest.”

Comprehensive and reliable data protection. To help meet RTO and RPO objectives in the remote and branch office, most disk-based solutions replace traditional nightly backup techniques with a more continuous form of data protection. Different solutions offer a variety of techniques to save copies of changed data to a protected disk, giving the user varying degrees of ability to recover to specific points-in-time.

In order to achieve comprehensive and reliable backup that will deliver the kind of granularity you need at recovery time, there are some key features to look for in a solution:

- Delta change engines that transmit only the data that changes in files and databases — a highly efficient approach that minimizes both server load and bandwidth usage and optimizes fast recovery; they may also offer snapshots and filters to reduce the impact on system performance.
- The ability to save those changes to an off-site location via an integrated online service.
- An efficient way of rolling up point-in-time windows and coalescing them into more comprehensive time frames — for example, multiple backups within a day into a single daily backup; multiple daily backups into monthly backups, etc.
- Checkpoint or point-in-time restart capability that automatically ensures that backup and restore jobs survive node failures and network resilience problems.
- Built-in protection (native support) for open files and databases — representing some of your business's most important data — enables backup of these files while they are in use, without disrupting your business flow.
- Make sure the solution not only backs up data but also allows you to back up *system information* — for easily restoring a full system when on-site technical staff is limited.
- The solution should offer customers flexibility in defining retention scheduling *and* policies for data on a per server or per folder basis, so that certain categories of data (e.g., financial) may be retained for years but others (e.g., CRM) for shorter time frames.
- A multi-tier architecture that allows greater freedom to drag and drop jobs onto redundant vaults — e.g., through RAIN technology (Redundant Array of Independent Nodes) that can provide fully automated data recovery in a local area network.

Ease of use. A fully automated disk-based backup and recovery solution requires minimal or no technical staff involvement — and allows remote server management from one location when desired.

- The service should be offered 24x7x365 to ensure backups are automatically performed accurately and completely around the clock — and transparently to the customer.
- Automated alerting should replace the requirement for users to manually monitor backup and recovery processes.
- When they choose to, authorized users should be able to manage and monitor the entire backup and recovery process anywhere and anytime. Online Web-based management should make it easy for the user to:
 - Create customized backup policies
 - Check status, audit jobs and users
 - Initiate restore operations
 - Retrieve all versions of data quickly through Web UI from catalog of historic versions
 - Create roles-based access levels for different types of users
 - Control archival requirements to ensure compliance with corporate and regulator guidelines

- The initial setup of the solution should be as painless as possible — not so complex that remote office requires special staff or a long time to learn and configure, as for example, solutions requiring additional products to extend and complete them or involving numerous components installed at various locations, adding additional steps to the set-up process. Ask references for their experience in deploying a particular solution.

Efficiency and speed. There are specific communications and storage techniques that facilitate fast recovery and promote cost control in disk-based backup and recovery:

- Previously mentioned as a feature under *Comprehensive and reliable data protection*, delta change engines transmit only the data that changes in files and databases, allowing recovery of a current version within minutes of a failure. Conversely, solutions that recopy entire files or require full system scans to detect changes will not be as efficient or fast.
- Bandwidth throttling with flexible scheduling allows businesses to control the amount of bandwidth used during any specified time to take better advantage of their existing infrastructure and minimize the impact backups have on other applications.
- Some solutions offer an optional appliance for local disk-speed recoveries of current data and recent history for recovering large amounts of data while meeting stringent Recovery Time Objectives.

Highly secure communications and storage. The level of security characterizing the disk-based backup and online service solution you choose is obviously critical to the success of your data protection strategy. Online service entails not only secure communications but also secure storage for data moved off-site.

- Look for resilient, efficient and secure communications provided over public and private connections both at the source where backup occurs *and* in transit to off-site storage.
- The type of encryption used (e.g., 256-bit AES encryption) should be clearly stated.
- At the source, data should be encrypted with a unique key defined by the customer. It's risky to rely on systems with only a single, massive key for entire vault (e.g., those reliant on checksums).
- To guard against forgetting or losing encryption keys, some solutions offer a password-protected, user-changeable, human-friendly encryption key built on top of machine-readable encryption key. As additional protection, there may be the option to escrow the key with the vendor.
- In transmitting the data, look for solutions that use the Secure Socket Layer (SSL) to establish a resilient, secure communication tunnel as the data travels to off-site storage.
- Finally, solutions that allow users to audit access to their administration management system provide added security as well as change control.

Vendor expertise and flexibility. Reliability is not only a technical attribute. There are other important questions that should be asked of any server backup and recovery solution provider that will help you evaluate their reliability so that you can select them with confidence:

- A managed service should be staffed by seasoned professionals who can provide proactive identification and solution of problems as they arise, without requiring the customer to monitor backup and recovery.
- Does the service provider guarantee successful data recovery in writing, for example, through an SLA?
- To what extent are data protection and storage the vendor's core competency? Ask the vendor how many millions of files their solution has restored to date — with an estimate of their recovery success rate. At

a minimum, they should be able to specify the number of sites at which their solution has been deployed and how long they have been running.

- Ask for a list of reference accounts to learn more about customers' experience with set up, implementation, and successful recoveries.
- The stability of the vendor's business is as important as the reliability of their solutions — particularly for service providers entrusted with all four aspects of your data protection workflow. Do their solutions address each step in that workflow: backup, removal, storage and recovery?
- Do they offer flexibility of choice through adjacent data protection and storage services that fit together with their server backup and recovery solution? For example:
 - Off-site tape vaulting services (which may already be used by the data center or larger locations across the business)
 - PC backup and recovery services and products that protect and defend data stored locally on desktops and mobile devices that may be lost or stolen
 - Protection and storage services for critical business information in various non-digital formats (e.g., paper and film) that must also be addressed by the business's data protection strategy to ensure regulatory compliance
- Managed services should offer simple, predictable pricing, with a guaranteed cost based on the amount of data to be protected on the customer's servers — rather than a variable cost that changes month to month based on circumstances outside the customer's control (changes in data compression, data change rate, success of backup, etc.).
- Use of a managed service from a third party offers instant scalability and requires no capital investment at the remote or branch office. For higher volumes of data, larger businesses with data centers may find it more cost-effective to obtain the solution as a licensed software product they install and manage themselves.
- In a licensed software product, look for a comprehensive solution with all the pieces developed by a single source — rather than a patchwork of partial solutions that require one another to address the full data protection workflow needs of the customer.
- Licensed products should not feature an excessive number of à la carte components — look for a comprehensive solution that addresses all parts of the data protection workflow, to avoid extra hidden cost.
- Avoid another source of hidden cost by ensuring that the solution does not require third party solutions to be added in (e.g., look for *native* support for open files and databases without complex plug-ins or costly third party tools).

NEXT STEPS IN EVALUATING DISK-BASED BACKUP FOR REMOTE AND BRANCH OFFICES

This paper has examined both the goals and the challenges for successfully protecting server data outside of a centralized data center, focusing on the specific needs and requirements of remote and branch offices. Solutions that combine disk-based backup with integrated online services offer these locations a viable alternative to traditional tape-based backup solutions. They address all the steps in the data protection workflow so that remote and branch offices can achieve a higher level of reliability, productivity and cost containment than is possible with more traditional backup methods.

Review your data protection strategy. Before undertaking an evaluation of these solutions, carefully review your overall data protection strategy. Simply to remedy an incomplete or expensive data protection program will not suffice unless it is done within the context of an overall business strategy. A piecemeal solution is *no* solution when it comes to data protection. A handy summary of *Best Practices to Secure and Protect Backup Data* is available on the Iron Mountain Web site⁴. These are grouped within five fundamental areas: assigning accountability, assessing risk, developing a data protection process, communicating the process and, finally, executing and testing the process.

Check out online resources. Iron Mountain's Web site also features real-life case studies of how other businesses have addressed their server data protection needs. Technical briefs and business advisories cover specific topics which may be of particular interest to you — for example, protecting open databases and files during disk-based backup, or securing protection specifically for Exchange servers.

Use the checklist. When you have reviewed your data protection strategy and learned about the best practices that characterize data protection practices and solutions, use the checklist provided to identify the server backup and recovery solution that best meets your specific needs. For additional information and assistance, please contact your Iron Mountain representative or email us at http://www.ironmountain.com/contact/contact_us.asp.

⁴ <http://www.ironmountain.com/US/digital/resources/>



745 Atlantic Avenue
Boston, Massachusetts 02111
(800) 899-IRON

Iron Mountain Digital, the world's leading provider of data backup/recovery and archiving software as a service (SaaS), offers a comprehensive suite of data protection and e-records management software and services to thousands of companies around the world. For more information, visit our Web site at www.ironmountain.com/digital.